

Amendment Under 37 C.F.R. § 1.111  
Attorney Docket No.: ST9-99-167 (A8117)  
U.S. Application No.: 09/513,065

## REMARKS

Claims 1-43 are all the claims pending in the application. By this Amendment, Applicant amends claims 1, 13 and 25 to further clarify the invention. Applicant also amends claims 5, 9-12, 17, 21-24, 29, 33-36 to conform these claims to the amended claims 1, 13 and 25. In addition, Applicant cancels claims 8, 20 and 32.

Furthermore, in order to provide more varied protection, Applicant adds claims 37-43. New claims 37-43 contain no impermissible new matter, and are clearly supported throughout the originally filed specification, e.g. see pages 5-7. Claims 37-42 are patentable over the prior art references cited by the Examiner at least by virtue of their dependency on independent claim 1. Claim 43 is patentable over the prior art references cited by the Examiner at least because of its recitations of “generating an authentication key based on a user name and a computer identifier...wherein said authentication key includes a user identifier for the computer connected to the data store.”

Applicant thanks the Examiner for withdrawing the previous rejection. The Examiner, however, found new grounds for rejecting claims 1-36. In particular, claims 1-4, 8, 10-16, 20, 22-28, 32, and 34-36 are rejected under 35 U.S.C. 103(a) as being unpatentable over Stallings Cryptography and Network Security 2<sup>nd</sup> Edition (hereinafter “Stallings”) in view of Bryant, “Designing an Authentication System: a Dialogue in Four Scenes” (hereinafter “Bryant”) and claims 5, 6, 7, 9, 17, 18, 19, 21, 29, 30, 31, and 33 are rejected under 35 U.S.C. 103(a) as being

Amendment Under 37 C.F.R. § 1.111  
Attorney Docket No.: ST9-99-167 (A8117)  
U.S. Application No.: 09/513,065

unpatentable over Stallings in view of Bryant and U.S. Patent No. 5,774,551 to Wu et al. (hereinafter “Wu”). Applicant respectfully traverses this rejection and respectfully requests the Examiner to reconsider this rejection in view of the following remarks.

Claims 8, 20 and 32 have been canceled. Therefore, this rejection with respect to these claims is literally moot. Of the remaining rejected claims, only claims 1, 13 and 25 are independent. This response will initially focus on these independent claims. Among a number of unique features of claim 1, not taught or suggested by the prior art, is “...generating an authentication key based on a user name and a computer identifier...wherein said authentication key includes a server user identifier.” The Examiner asserts that claim 1 is directed to a user authentication method and is obvious over Stalling and Bryant. The Examiner asserts that Bryant teaches including a network address to the ticket and that Stalling’s teaches all other features of claim 1 (see pages 2-3 of the Office Action). Applicant has carefully studied Stalling’s discussion of the Kerberos method and Bryant’s dramatical dialogue of the Kerberos system. Taken alone or in any conceivable combination, these teachings are not similar to “...generating an authentication key based on a user name and a computer identifier...wherein said authentication key includes a server user identifier.”

In the conventional unified logon systems, each client computer connected to a database server computer needs to have a corresponding user identifier and password created on the server computer, in addition to having a user name and a password to log onto the client computer. This requirement creates an administrative nightmare because of maintaining and managing all the client user names and passwords with the corresponding server user IDs and passwords.

Moreover, when a server password or ID is changed, the system administrator needs to notify the users of their new password or server ID, creating additional security risk of the message being intercepted by hackers. In the method as set forth in claim 1, however, the authentication key is generated “based on a user name and a computer identifier” and the authentication key “includes a server user identifier.” As a result, the administrator need not forward the server ID to the user. Instead, the server ID is sent to the user in an authentication key based only on the user name and a computer identifier received from the user.

Stallings, similar to the conventional techniques described above, teaches a client sending a server ID, along with the client name and password. These server ID, client ID and client password are encrypted by the authentication system to create a ticket for the client. The client then uses this ticket to gain access to the server. The server verifies client ID with the encrypted client ID in the ticket. If the two match, access to server is provided (page 326 of Stallings). This is no different from the conventional techniques described in the background of the invention. When the administrator changes the server ID, a new server ID has to be sent to the user, creating additional security risk of the message being intercepted by hackers.

Bryant, is no different from Stallings, except that Bryant’s ticket includes a network address of the client computer, which is checked against the network address of the client, which sent the ticket (page 5 of Bryant). Thus, this design guards against the interception of the ticket and attempts to send it from a different computer. Bryant, however, fails to address the problem of changing server IDs for the user. Moreover, Bryant is a dialogue suggesting theoretical

Amendment Under 37 C.F.R. § 1.111  
Attorney Docket No.: ST9-99-167 (A8117)  
U.S. Application No.: 09/513,065

design for the authentication system. Bryant does not teach or suggest the actual implementation of the system, which would include the network addresses.

Therefore, "...generating an authentication key based on a user name and a computer identifier...wherein said authentication key includes a server user identifier," as set forth in claim 1 is not suggested or taught by the combined teachings of Stallings and Bryant, which lack having the user only send the user name and a computer identifier and receive a ticket with the server ID. Together, the combined teachings of these references would not have (and could not have) led the artisan of ordinary skill to have achieved the subject matter of claim 1. Since claims 1-4 and 10-12 are dependent upon claim 1, they may be patentable at least by virtue of their dependency.

Next, Applicant respectfully traverses this rejection with respect to independent claims 13 and 25. These independent claims, as now amended, recite: "generating an authentication key that includes a server user name based on a user name and a computer identifier." This recitation is similar to the features argued above with respect to claim 1. Therefore, those arguments are respectfully submitted to apply with equal force here. For at least substantially the same reasons, therefore, Applicant respectfully requests the Examiner to withdraw this rejection of independent claims 13 and 25. Claims 14-16 and 22-24, and claims 26-28 and 34-36 are patentable at least by virtue of their dependency on claims 13 and 25, respectively.

In addition, dependent claims 12, 24, and 36 recite: "intercepting the authentication key; and if the user name and a computer identifier are valid, logging onto the server." The Examiner

Amendment Under 37 C.F.R. § 1.111  
Attorney Docket No.: ST9-99-167 (A8117)  
U.S. Application No.: 09/513,065

alleges that claim 12, for example, does not teach or define anything more than the features claimed in claims 1-3 and therefore is rejected for the same reasons (see page 6 of the Office Action). Applicant respectfully disagrees. Claim 12 recites “intercepting the authentication key”. Both Stallings and Bryant fails to teach or suggest interception of the key. In Stallings and Bryant, the client receives from an authentication system a ticket. This ticket is sent directly to the server for access to that server. Both Stallings and Bryant fail to teach or suggest, interception of this ticket. Moreover, the ticket is not processed by the authentication system but by the server to which this ticket was sent. In short, for at least this additional reason, dependent claims 12, 24 and 36 are patentable over the combined teachings of Stallings and Bryant.

Dependent claims 5, 6, 7, 9, 17, 18, 19, 21, 29, 30, 31, and 33 are rejected under 35 U.S.C. 103(a) as being unpatentable over Stallings in view of Bryant and Wu. Applicant respectfully traverses this rejection with respect to claims 5, 6, 7, 9, 17, 18, 19, 21, 29, 30, 31, and 33, which depend on independent claim 1, 13 or 25. Applicant has already demonstrated that the combined teachings of Stallings and Bryant do not meet all the requirements of independent claims 1, 13 and 25. Wu is relied upon only for its teaching of unified login to a plurality of services having their own authentication restrictions (see pages 7-8 of the Office Action). In particular, the Examiner alleges that having Wu’s method of stacking account management services by having primary and secondary authentication services is similar to “generating an authentication key based on the user name and computer identifier...wherein the authentication key includes a server identifier,” as set forth in the independent claims 1, 13 and 25.

Applicant has carefully studied Wu's discussion of primary and secondary authentication tokens, and Applicant respectfully submits, that Wu, taken alone or in any conceivable combination with the teachings of Stallings and Bryant, are not similar to "generating an authentication key that includes a server user name based on a user name and a computer identifier."

Wu teaches a unified login process by using an authentication token mapping process. This process uses a user's primary authentication token for a primary authentication service, such as a password, private key, or other unique data, to encrypt the user's other authentication tokens for other secondary authentication services (col. 3, lines 55 to 62). That is, Wu teaches a method to set up user credentials in the Kerberos environment. In particular, when user is connecting to a server, the authentication interface 123 first checks whether the name and address of the remote computer against a list of trusted remote computers. If the remote computer is not trusted, the user's handle and the primary authentication token is passed to the selected authentication services. After authentication, the credential is a ticket for accessing a ticket granting service. The ticket may include the user id and group id information in the encrypted form (col. 13, line 35 to col. 14, line 28). The encrypted authentication tokens, along with data indicating which authentication services they are associated with, are stored in an available storage facility, such as a user context, naming service, smart card, or the like. In this manner, the user need only remember or provide a single authentication token to the computer system, even though multiple authentication services are supported (col. 3, line 62 to col. 4, line 2).

Amendment Under 37 C.F.R. § 1.111  
Attorney Docket No.: ST9-99-167 (A8117)  
U.S. Application No.: 09/513,065

Wu, however, teaches having a primary authentication token to encrypt other secondary tokens, storing secondary and primary tokens in a user storage facility (col. 10, line 38 to col. 11, line 55). Wu fails to teach or suggest “generating an authentication key that includes a server user name based on a user name and a computer identifier.” In Wu, the primary token only includes user identity received from the user, and the secondary tokens are generated based on this primary, encrypted token. In short, Wu does not compensate for the deficient teachings of Stallings and Bryant. Together, the combined teachings of these references would not have (and could not have) led the artisan of ordinary skill to have achieved the subject matter of independent claims 1, 13 and 25. Since claims 5, 6, 7, 9, 17, 18, 19, 21, 29, 30, 31, and 33 are dependent upon claim 1, 13 or 25, they may be patentable at least by virtue of their dependency.

In view of the above, reconsideration and allowance of this application are now believed to be in order, and such actions are hereby solicited. If any points remain in issue which the Examiner feels may be best resolved through a personal or telephone interview, the Examiner is kindly invited to contact the undersigned attorney at the telephone number listed below.

Amendment Under 37 C.F.R. § 1.111  
Attorney Docket No.: ST9-99-167 (A8117)  
U.S. Application No.: 09/513,065

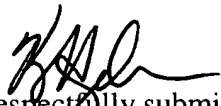
The USPTO is directed and authorized to charge all required fees, except for the Issue Fee and the Publication Fee, to Deposit Account No. 19-4880. Please also credit any overpayments to said Deposit Account.

SUGHRUE MION, PLLC  
Telephone: (202) 293-7060  
Facsimile: (202) 293-7860

WASHINGTON OFFICE

**23373**

CUSTOMER NUMBER

  
Respectfully submitted,  
Kelly G. Hyndman  
Registration No. 39,234  
William H. Mandir  
Registration No. 32,156

Date: May 25, 2004